

# Previous

```
247 ((void (__usercall *)(unsigned int@<ecx>, wchar_t *, wchar_t *, int))custom_strncpy)(
248 v41,
249 concatURL_addr,
250 v47,
251 v46 + 1);
252
253 {
254
255     v31 = ((int (__usercall *)@<eax>(wchar_t *@<ecx>, char *, int))sub_25818D6E)(
256         v30,
257         (char *)concatURL_addr,
258         '/');
259     if ( v31 )
260         *(_BYTE *) (v31 + 1) = 0;
261     else
262         *(_BYTE *)concatURL_addr = 0;
263 }
264
265 if ( v58 )
266 {
267     len_allocaddr = (int)custom_strlen((LPCSTR)concatURL_addr);
268     ((void (__usercall *)(uintptr_t@<ecx>, char *, char *, int))custom_strncat)(
269         v58 + 1,
270         (char *)concatURL_addr,
271         v59,
272         v58 + 1 + len_allocaddr);
273 }
274 sub_25802E0C((int)concatURL_addr, 0);
275
```

취약한 문자열 연결 함수를 호출하기 전에 연결 URL을 저장할 heap에 base URL 복사해서 저장함

```
((void (__usercall *)(unsigned int@<ecx>, wchar_t *, wchar_t *, int))custom_strncpy)(
v41,
concatURL_addr,
v47,
v46 + 1);
```

Base URL

0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42
------	------	------	------	------	------	------	------	------	------

Concat URL

0xFE	0xFF	0x41	0x41	0x00	0x00				
------	------	------	------	------	------	--	--	--	--

# Normal

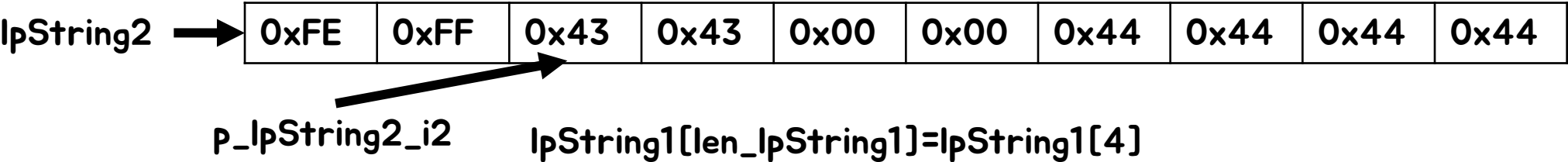
len\_lpString1 : 4

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        lpString2_i2 = *p_lpString2_i2;
        p_lpString2_i2 += 2;
        *concatpoint = lpString2_i2;
        concatpoint += 2;
        lpString2_i3 = *(p_lpString2_i2 - 1);
        *(concatpoint - 1) = lpString2_i3;
    }
    while ( lpString2_i2 );
    while ( lpString2_i3 );
}
```

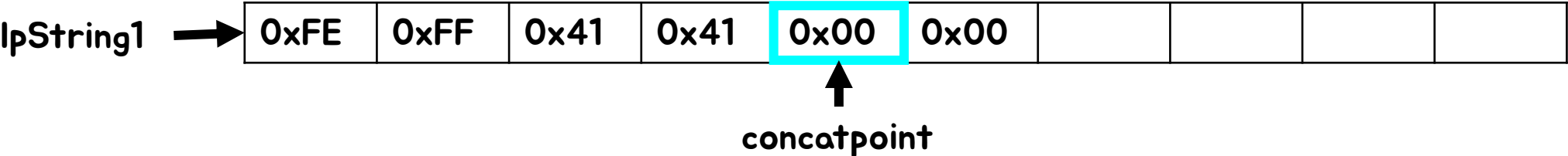
Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL



Concat URL



# Normal

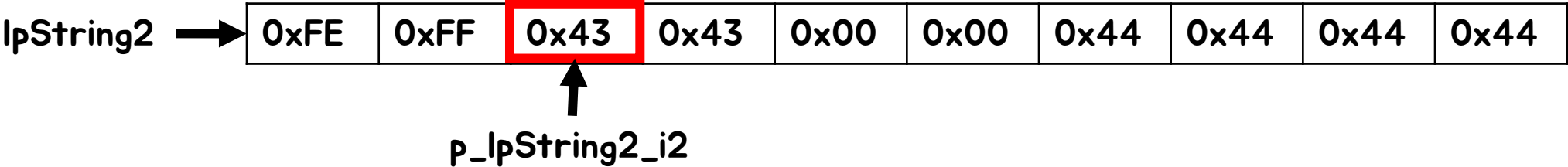
```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            *concatpoint = lpString2_i2;
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x43  
lpString2\_i3 :

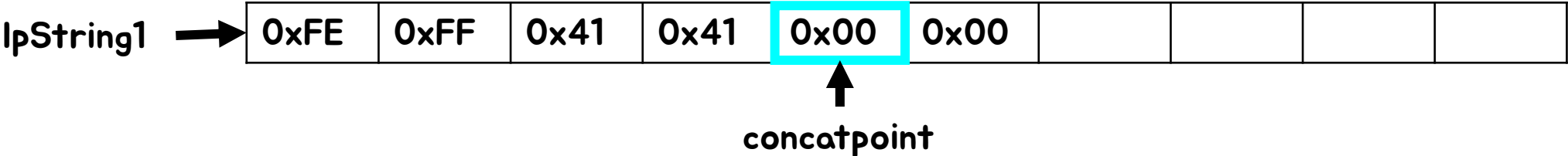
Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL



Concat URL



# Normal

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i3 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            concatpoint = lpString2_i2;
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x43  
lpString2\_i3 :

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0xFE	0xFF	0x43	0x43	0x00	0x00	0x44	0x44	0x44	0x44
------	------	------	------	------	------	------	------	------	------

↑  
p\_lpString2\_i2

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x00	0x00				
------	------	------	------	------	------	--	--	--	--

↑  
concatpoint

# Normal

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 = p_lpString2_i2 + 1;
            *concatpoint = lpString2_i2;
            concatpoint++;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x43  
lpString2\_i3 :

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0xFE	0xFF	0x43	0x43	0x00	0x00	0x44	0x44	0x44	0x44
------	------	------	------	------	------	------	------	------	------

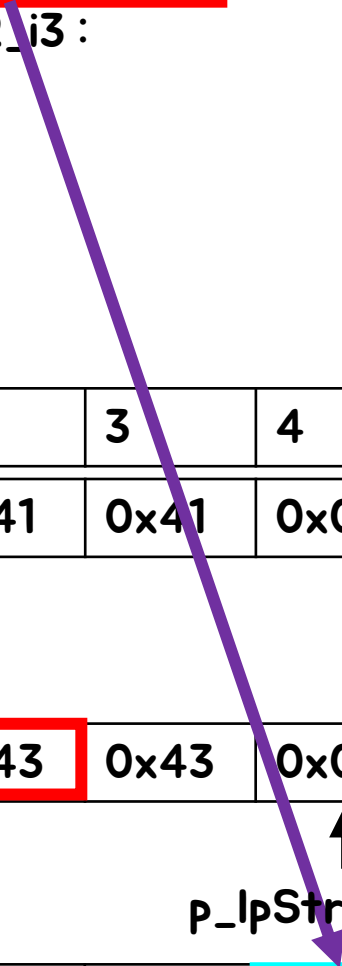
p\_lpString2\_i2 ↑

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x43	0x00				
------	------	------	------	------	------	--	--	--	--

concatpoint ↑



# Normal

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            *concatpoint = lpString2_i2;
            concatpoint += 2;
            p_lpString2_i2 = (p_lpString2_i2 + 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x43  
lpString2\_i3 :

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0xFE	0xFF	0x43	0x43	0x00	0x00	0x44	0x44	0x44	0x44
------	------	------	------	------	------	------	------	------	------

↑  
p\_lpString2\_i2

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x43	0x00				
------	------	------	------	------	------	--	--	--	--

↑  
concatpoint

# Normal

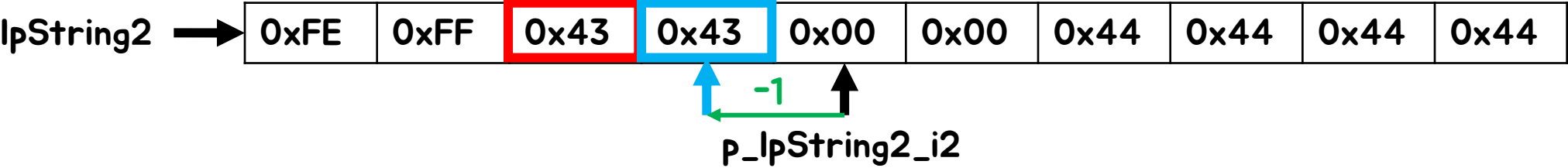
```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            *concatpoint = lpString2_i2;
            concatpoint++;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            (concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x43  
lpString2\_i3 : 0x43

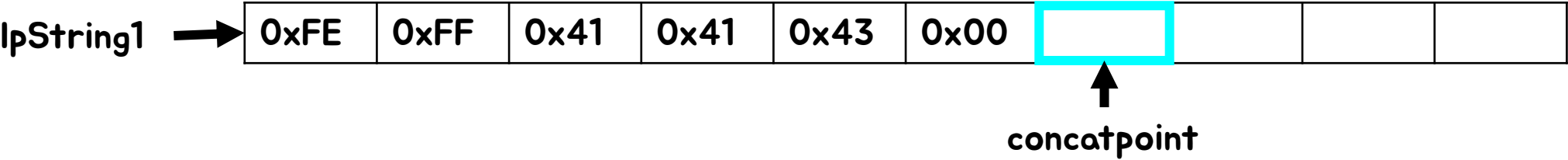
Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL



Concat URL



# Normal

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            *concatpoint = lpString2_i2;
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
**lpString2\_i2 : 0x43**  
**lpString2\_i3 : 0x43**

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0xFE	0xFF	<b>0x43</b>	<b>0x43</b>	0x00	0x00	0x44	0x44	0x44	0x44
------	------	-------------	-------------	------	------	------	------	------	------

↑  
p\_lpString2\_i2

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x43	<b>0x43</b>				
------	------	------	------	------	-------------	--	--	--	--

← -1 ↑  
concatpoint



# Normal

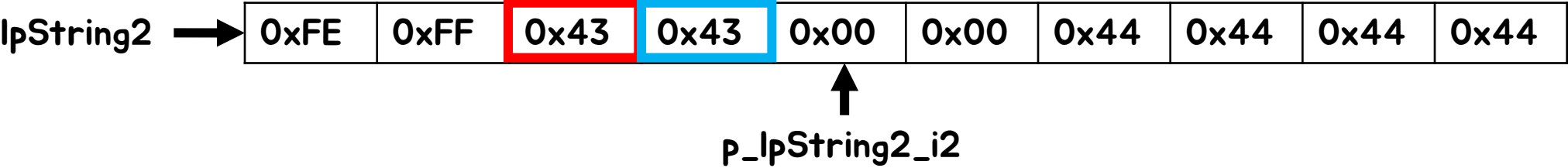
```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            *concatpoint = lpString2_i2;
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x43 != 0x00  
lpString2\_i3 : 0x43

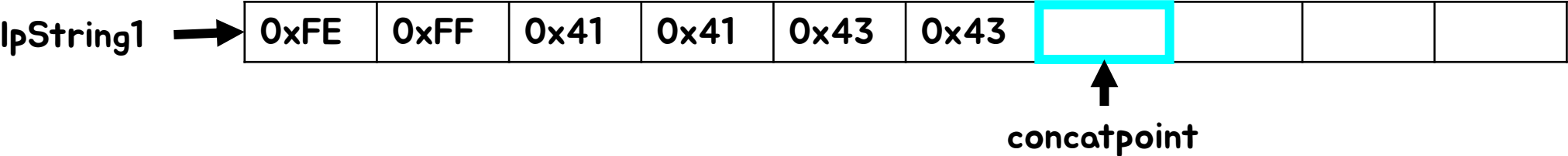
Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL



Concat URL



# Normal

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2++;
            *concatpoint = lpString2_i2;
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x00  
lpString2\_i3 : 0x43

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0xFE	0xFF	0x43	0x43	0x00	0x00	0x44	0x44	0x44	0x44
------	------	------	------	------	------	------	------	------	------

↑  
p\_lpString2\_i2

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x43	0x43				
------	------	------	------	------	------	--	--	--	--

↑  
concatpoint

# Normal

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i3 = *lpString2_i2;
            p_lpString2_i2 += 2;
            concatpoint = lpString2_i2;
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x00  
lpString2\_i3 : 0x43

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0xFE	0xFF	0x43	0x43	0x00	0x00	0x44	0x44	0x44	0x44
------	------	------	------	------	------	------	------	------	------

↑  
p\_lpString2\_i2

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x43	0x43				
------	------	------	------	------	------	--	--	--	--

↑  
concatpoint

# Normal

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            *concatpoint = lpString2_i2;
            concatpoint++;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x00  
lpString2\_i3 : 0x43

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0xFE	0xFF	0x43	0x43	0x00	0x00	0x44	0x44	0x44	0x44
------	------	------	------	------	------	------	------	------	------

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x43	0x43	0x00			
------	------	------	------	------	------	------	--	--	--

p\_lpString2\_i2

concatpoint

# Normal

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            *lpString2_i3 = lpString2_i2;
            concatpoint += 2;
            p_lpString2_i2 = (p_lpString2_i2 + 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x00  
lpString2\_i3 : 0x43

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0xFE	0xFF	0x43	0x43	0x00	0x00	0x44	0x44	0x44	0x44
------	------	------	------	------	------	------	------	------	------

↑  
p\_lpString2\_i2

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x43	0x43	0x00			
------	------	------	------	------	------	------	--	--	--

↑  
concatpoint

# Normal

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            *concatpoint = lpString2_i2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            (concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x00  
lpString2\_i3 : 0x00

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0xFE	0xFF	0x43	0x43	0x00	0x00	0x44	0x44	0x44	0x44
------	------	------	------	------	------	------	------	------	------



p\_lpString2\_i2

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x43	0x43	0x00			
------	------	------	------	------	------	------	--	--	--



concatpoint

# Normal

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            *concatpoint = lpString2_i2;
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 + 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
**lpString2\_i2 : 0x00**  
**lpString2\_i3 : 0x00**

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0xFE	0xFF	0x43	0x43	<b>0x00</b>	<b>0x00</b>	0x44	0x44	0x44	0x44
------	------	------	------	-------------	-------------	------	------	------	------

p\_lpString2\_i2 ↑

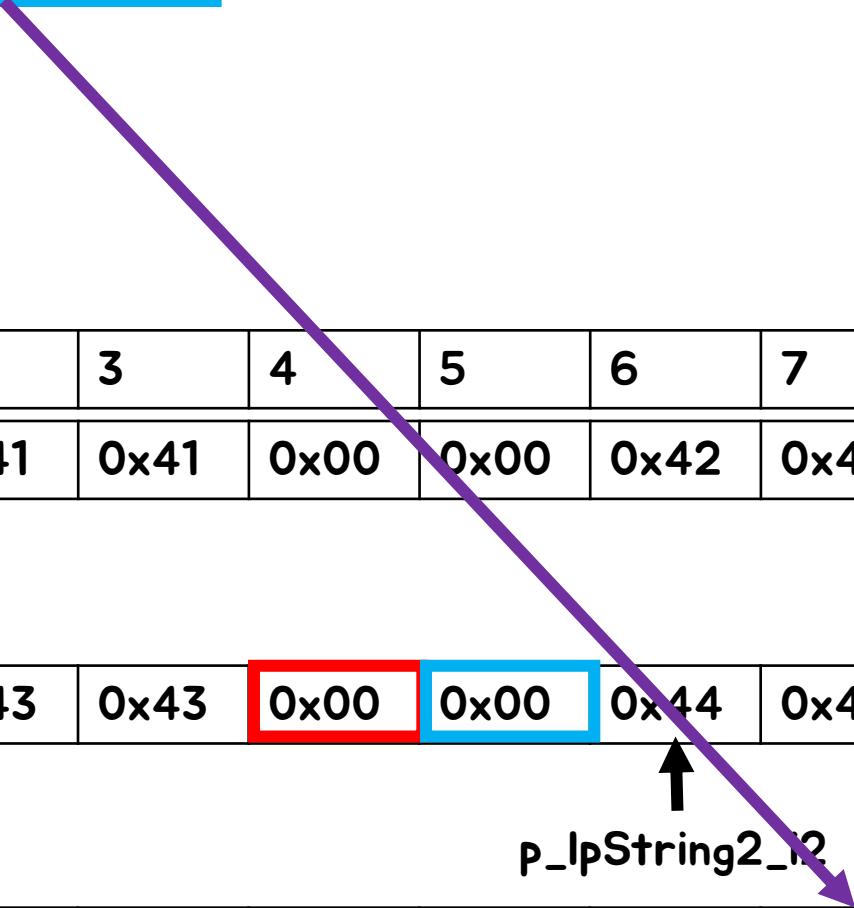
Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x43	0x43	0x00	0x00		
------	------	------	------	------	------	------	------	--	--

← -1

concatpoint ↑



# Normal

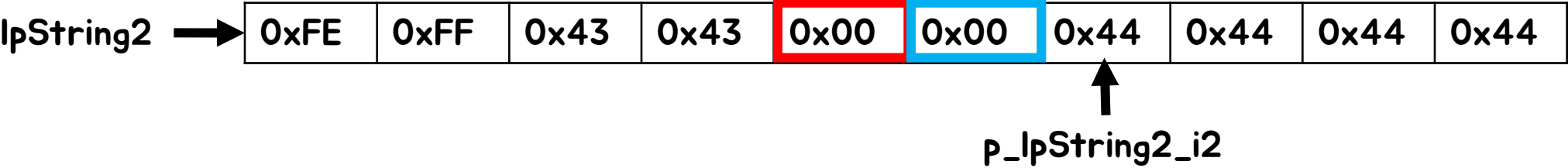
```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            *concatpoint = lpString2_i2;
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x00 == 0x00  
lpString2\_i3 : 0x00

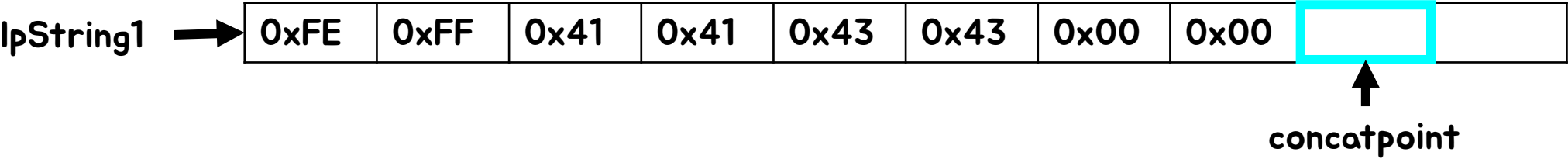
Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL



Concat URL





# Normal

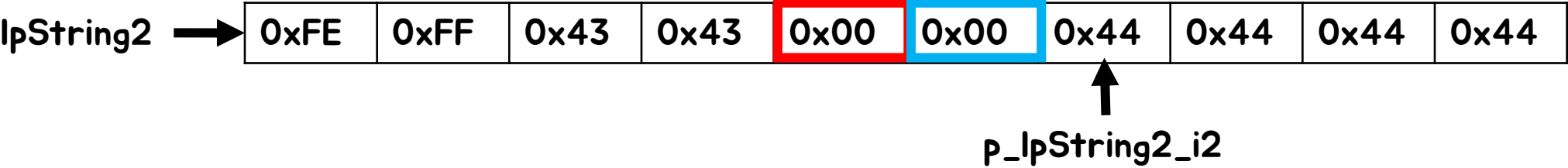
```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            *concatpoint = lpString2_i2;
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x00 == 0x00  
lpString2\_i3 : 0x00 == 0x00

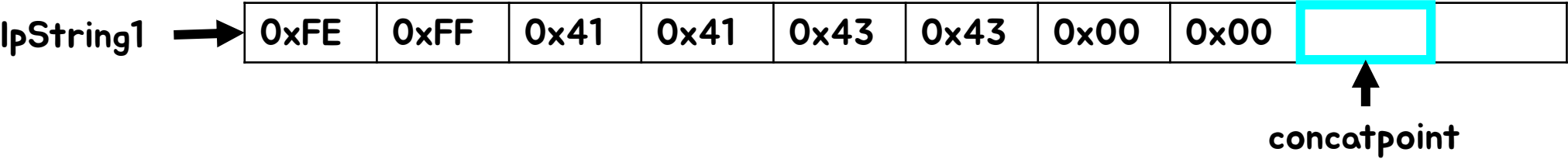
Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL



Concat URL



# Normal

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            *concatpoint = lpString2_i2;
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x00 == 0x00  
lpString2\_i3 : 0x00 == 0x00

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0xFE	0xFF	0x43	0x43	0x00	0x00	0x44	0x44	0x44	0x44
------	------	------	------	------	------	------	------	------	------

↑  
p\_lpString2\_i2

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x43	0x43	0x00	0x00		
------	------	------	------	------	------	------	------	--	--

↑  
concatpoint

# Root Cause

len\_lpString1 : 4

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        lpString2_i2 = *p_lpString2_i2;
        p_lpString2_i2 += 2;
        *concatpoint = lpString2_i2;
        concatpoint += 2;
        lpString2_i3 = *(p_lpString2_i2 - 1);
        *(concatpoint - 1) = lpString2_i3;
    }
    while ( lpString2_i2 );
    while ( lpString2_i3 );
}
```

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0x12	0x34	0x56	0x78	0x90	0x00	0x11	0x22	0x00	0x00
------	------	------	------	------	------	------	------	------	------

p\_lpString2\_i2

lpString1[len\_lpString1]=lpString1[4]

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x00	0x00				
------	------	------	------	------	------	--	--	--	--

concatpoint

# Root Cause

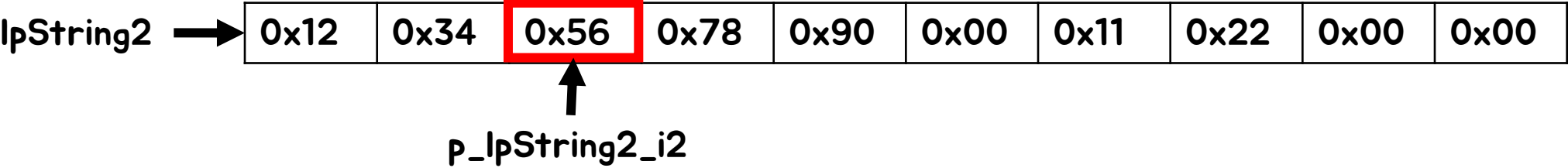
```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            *concatpoint = lpString2_i2;
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x56  
lpString2\_i3 :

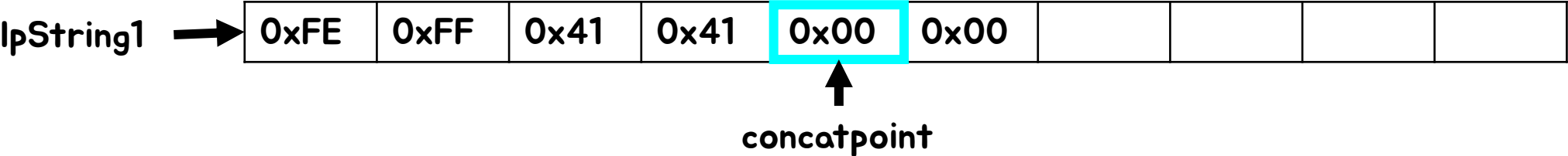
Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL



Concat URL



# Root Cause

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i3 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            concatpoint = &lpString1[concatpoint - 1];
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x56  
lpString2\_i3 :

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0x12	0x34	0x56	0x78	0x90	0x00	0x11	0x22	0x00	0x00
------	------	------	------	------	------	------	------	------	------

↑  
p\_lpString2\_i2

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x00	0x00				
------	------	------	------	------	------	--	--	--	--

↑  
concatpoint

# Root Cause

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 = p_lpString2_i2 + 2;
            *concatpoint = lpString2_i2;
            concatpoint++;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
**lpString2\_i2 : 0x56**  
lpString2\_i3 :

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0x12	0x34	<b>0x56</b>	0x78	0x90	0x00	0x11	0x22	0x00	0x00
------	------	-------------	------	------	------	------	------	------	------

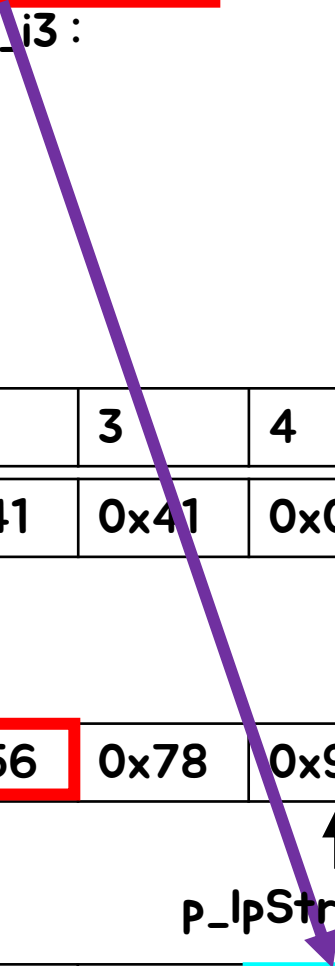
p\_lpString2\_i2

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	<b>0x56</b>	0x00				
------	------	------	------	-------------	------	--	--	--	--

concatpoint



# Root Cause

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            *concatpoint = lpString2_i2;
            concatpoint += 2;
            p_lpString2_i2 = (p_lpString2_i2 + 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x56  
lpString2\_i3 :

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0x12	0x34	0x56	0x78	0x90	0x00	0x11	0x22	0x00	0x00
------	------	------	------	------	------	------	------	------	------

↑  
p\_lpString2\_i2

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x56	0x00				
------	------	------	------	------	------	--	--	--	--

↑  
concatpoint

# Root Cause

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            *concatpoint = lpString2_i2;
            concatpoint++;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            (concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x56  
lpString2\_i3 : 0x78

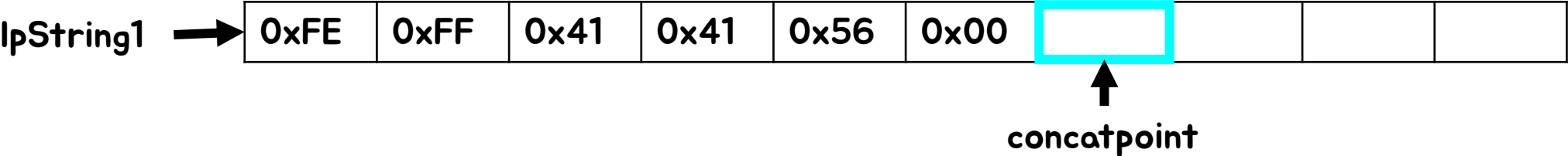
Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL



Concat URL





# Root Cause

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            *concatpoint = lpString2_i2;
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
**lpString2\_i2 : 0x56**  
**lpString2\_i3 : 0x78**

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0x12	0x34	<b>0x56</b>	<b>0x78</b>	0x90	0x00	0x11	0x22	0x00	0x00
------	------	-------------	-------------	------	------	------	------	------	------

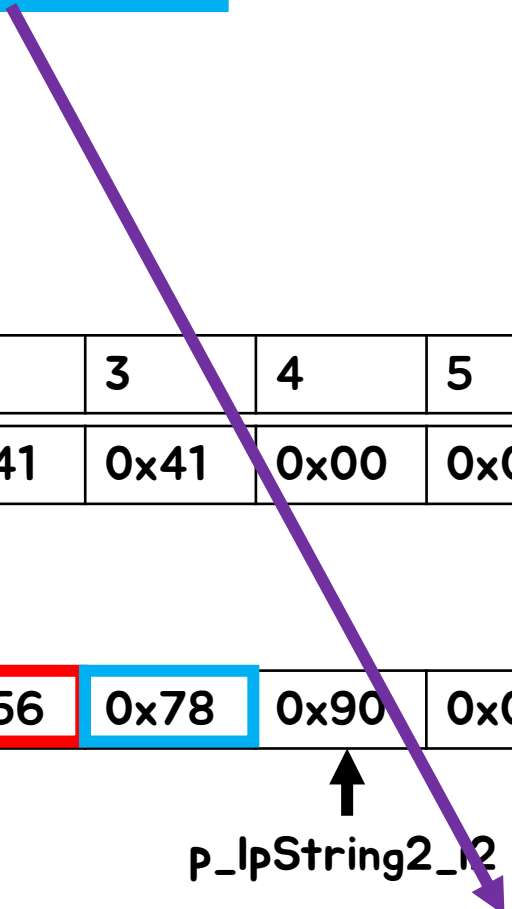
↑  
p\_lpString2\_i2

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x56	0x78				
------	------	------	------	------	------	--	--	--	--

↑ -1  
concatpoint



# Root Cause

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            *concatpoint = lpString2_i2;
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x56 != 0x00  
lpString2\_i3 : 0x78

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0x12	0x34	0x56	0x78	0x90	0x00	0x11	0x22	0x00	0x00
------	------	------	------	------	------	------	------	------	------

↑  
p\_lpString2\_i2

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x56	0x78				
------	------	------	------	------	------	--	--	--	--

↑  
concatpoint

# Root Cause

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2++;
            *concatpoint = lpString2_i2;
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x90  
lpString2\_i3 : 0x78

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0x12	0x34	0x56	0x78	0x90	0x00	0x11	0x22	0x00	0x00
------	------	------	------	------	------	------	------	------	------

p\_lpString2\_i2

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x56	0x78				
------	------	------	------	------	------	--	--	--	--

concatpoint

# Root Cause

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i3 = *lpString2_i2;
            p_lpString2_i2 += 2;
            concatpoint = lpString2_i2;
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x90  
lpString2\_i3 : 0x78

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0x12	0x34	0x56	0x78	0x90	0x00	0x11	0x22	0x00	0x00
------	------	------	------	------	------	------	------	------	------

↑  
p\_lpString2\_i2

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x56	0x78				
------	------	------	------	------	------	--	--	--	--

↑  
concatpoint

# Root Cause

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            *concatpoint = lpString2_i2;
            concatpoint++;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x90  
lpString2\_i3 : 0x78

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0x12	0x34	0x56	0x78	0x90	0x00	0x11	0x22	0x00	0x00
------	------	------	------	------	------	------	------	------	------

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x56	0x78	0x90			
------	------	------	------	------	------	------	--	--	--

p\_lpString2\_i2

concatpoint

# Root Cause

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            *lpString2_i3 = *p_lpString2_i2;
            concatpoint += 2;
            p_lpString2_i2 = (p_lpString2_i2 + 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x90  
lpString2\_i3 : 0x78

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0x12	0x34	0x56	0x78	0x90	0x00	0x11	0x22	0x00	0x00
------	------	------	------	------	------	------	------	------	------

↑  
p\_lpString2\_i2

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x56	0x78	0x90			
------	------	------	------	------	------	------	--	--	--

↑  
concatpoint

# Root Cause

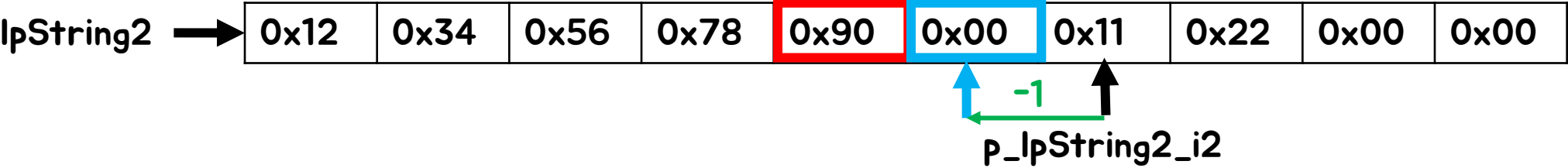
```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            *concatpoint = lpString2_i2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            (concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x90  
lpString2\_i3 : 0x00

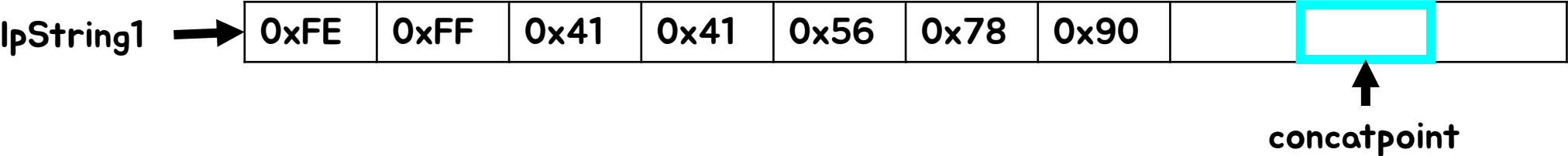
Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL



Concat URL



# Root Cause

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            *concatpoint = lpString2_i2;
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
**lpString2\_i2 : 0x90**  
**lpString2\_i3 : 0x00**

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0x12	0x34	0x56	0x78	<b>0x90</b>	<b>0x00</b>	0x11	0x22	0x00	0x00
------	------	------	------	-------------	-------------	------	------	------	------

p\_lpString2\_i2

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x56	0x78	0x90	0x00		
------	------	------	------	------	------	------	------	--	--

concatpoint

-1



# Root Cause

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            *concatpoint = lpString2_i2;
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x90 != 0x00  
lpString2\_i3 : 0x00

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0x12	0x34	0x56	0x78	0x90	0x00	0x11	0x22	0x00	0x00
------	------	------	------	------	------	------	------	------	------

↑  
p\_lpString2\_i2

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x56	0x78	0x90	0x00		
------	------	------	------	------	------	------	------	--	--

↑  
concatpoint

# Root Cause

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2++;
            *concatpoint = lpString2_i2;
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x11  
lpString2\_i3 : 0x00

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0x12	0x34	0x56	0x78	0x90	0x00	0x11	0x22	0x00	0x00
------	------	------	------	------	------	------	------	------	------

↑  
p\_lpString2\_i2

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x56	0x78	0x90	0x00		
------	------	------	------	------	------	------	------	--	--

↑  
concatpoint

# Root Cause

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i3 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x11  
lpString2\_i3 : 0x00

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0x12	0x34	0x56	0x78	0x90	0x00	0x11	0x22	0x00	0x00
------	------	------	------	------	------	------	------	------	------

↑  
p\_lpString2\_i2

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x56	0x78	0x90	0x00		
------	------	------	------	------	------	------	------	--	--

↑  
concatpoint

# Root Cause

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            *concatpoint = lpString2_i2;
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x11  
lpString2\_i3 : 0x00

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

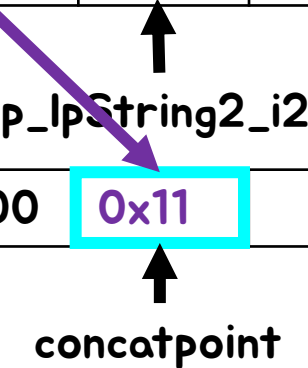
lpString2 →

0x12	0x34	0x56	0x78	0x90	0x00	0x11	0x22	0x00	0x00
------	------	------	------	------	------	------	------	------	------

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x56	0x78	0x90	0x00	0x11	
------	------	------	------	------	------	------	------	------	--



# Root Cause

```
if ( *lpString1 == (CHAR)0xFF && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            *concatpoint = *lpString2_i2;
            concatpoint += 2;
            lpString2_i2 = (p_lpString2_i2 + 2);
            *(concatpoint - 1) = lpString2_i3;
        } while ( lpString2_i2 );
    } while ( lpString2_i3 );
}
```

**len\_lpString1 : 4**

**lpString2\_i2 : 0x11**

**lpString2\_i3 : 0x00**

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

## Relative URL

## IpString2

0x12	0x34	0x56	0x78	0x90	0x00	0x11	0x22	0x00	0x00
------	------	------	------	------	------	------	------	------	------

p\_lpString2\_i2

## Concat URL

## lpString1

[illegible]

## concatpoint

# Root Cause

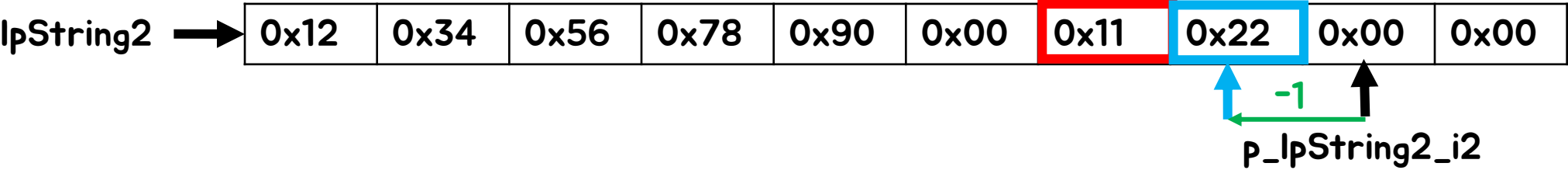
```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            *concatpoint = lpString2_i2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            (concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x11  
lpString2\_i3 : 0x22

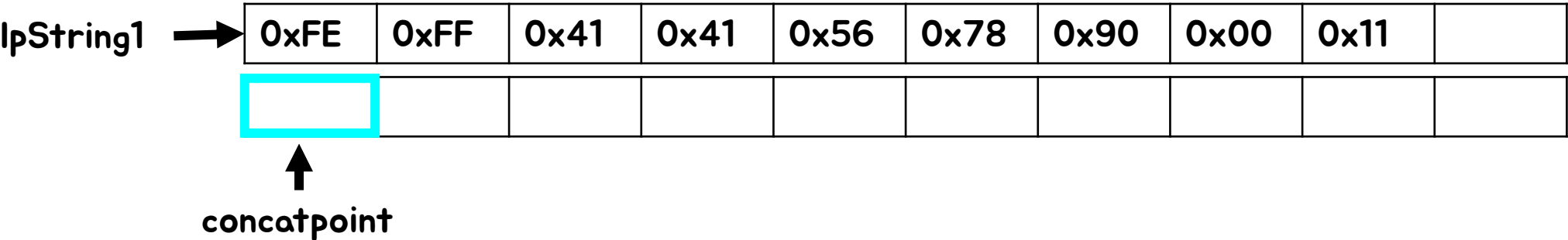
Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL



Concat URL



# Root Cause

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            *concatpoint = lpString2_i2;
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 + 1);
        } while ( lpString2_i2 );
        while ( lpString2_i3 );
        *(concatpoint - 1) = lpString2_i3;
    }
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x11  
lpString2\_i3 : 0x22

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0x12	0x34	0x56	0x78	0x90	0x00	0x11	0x22	0x00	0x00
------	------	------	------	------	------	------	------	------	------

p\_lpString2\_i2

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x56	0x78	0x90	0x00	0x11	0x22

-1  
concatpoint

# Root Cause

```
if ( *lpString1 == (CHAR)0xFF && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        lpString2_i2 = *p_lpString2_i2;
        p_lpString2_i2 += 2;
        *concatpoint = lpString2_i2;
        concatpoint += 2;
        lpString2_i3 = *(p_lpString2_i2 - 1);
        *(concatpoint - 1) = lpString2_i3;
    }
    while ( lpString2_i2 );
    while ( lpString2_i3 );
}
```

```
len_lpString1 : 4
lpString2_i2 : 0x11 != 0x00
lpString2_i3 : 0x22
```

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

## Base URL

## Relative URL

## IpString2

0x12	0x34	0x56	0x78	0x90	0x00	0x11	0x22	0x00	0x00
------	------	------	------	------	------	------	------	------	------

p\_lpString2\_i2

## Concat URL

## IpString1

0xFE	0xFF	0x41	0x41	0x56	0x78	0x90	0x00	0x11	0x22

## concatpoint



# Root Cause

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2++;
            *concatpoint = lpString2_i2;
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

```
len_lpString1 : 4
lpString2_i2 : 0x00
lpString2_i3 : 0x22
```

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

## Base URL

## Relative URL

## IpString2

0x12	0x34	0x56	0x78	0x90	0x00	0x11	0x22	0x00	0x00
------	------	------	------	------	------	------	------	------	------

p\_lpString2\_i2

## Concat URL

## lpString1

[illegible]

## concatpoint

# Root Cause

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i3 = *lpString2_i2;
            p_lpString2_i2 += 2;
            concatpoint = lpString2_i2;
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x00  
lpString2\_i3 : 0x22

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0x12	0x34	0x56	0x78	0x90	0x00	0x11	0x22	0x00	0x00
------	------	------	------	------	------	------	------	------	------

p\_lpString2 ↑

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x56	0x78	0x90	0x00	0x11	0x22

concatpoint ↑

# Root Cause

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            // lpString2_i3 = *p_lpString2_i3;
            *concatpoint = lpString2_i2;
            // concatpoint++;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x00  
lpString2\_i3 : 0x22

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0x12	0x34	0x56	0x78	0x90	0x00	0x11	0x22	0x00	0x00
------	------	------	------	------	------	------	------	------	------

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x56	0x78	0x90	0x00	0x11	0x22
0x00									

concatpoint

p\_lpString

# Root Cause

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            *p_lpString2_i3 = lpString2_i2;
            concatpoint += 2;
            p_lpString2_i2 = (p_lpString2_i2 + 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x00  
lpString2\_i3 : 0x22

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0x12	0x34	0x56	0x78	0x90	0x00	0x11	0x22	0x00	0x00
------	------	------	------	------	------	------	------	------	------

p\_lpString2 ↑

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x56	0x78	0x90	0x00	0x11	0x22
0x00									



concatpoint

# Root Cause

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            *concatpoint = lpString2_i2;
            concatpoint++;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            (concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x00  
lpString2\_i3 : 0x00

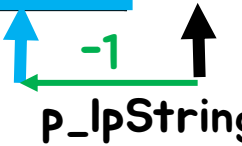
Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0x12	0x34	0x56	0x78	0x90	0x00	0x11	0x22	0x00	0x00
------	------	------	------	------	------	------	------	------	------



Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x56	0x78	0x90	0x00	0x11	0x22
0x00									



concatpoint

# Root Cause

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            *concatpoint = lpString2_i2;
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 + 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
**lpString2\_i2 : 0x00**  
**lpString2\_i3 : 0x00**

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0x12	0x34	0x56	0x78	0x90	0x00	0x11	0x22	<b>0x00</b>	<b>0x00</b>
------	------	------	------	------	------	------	------	-------------	-------------

p\_lpString2 ↑

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x56	0x78	0x90	0x00	0x11	0x22
0x00	0x00								

**concatpoint**  
↑ -1

# Root Cause

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            *concatpoint = lpString2_i2;
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x00 == 0x00  
lpString2\_i3 : 0x00

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0x12	0x34	0x56	0x78	0x90	0x00	0x11	0x22	0x00	0x00
------	------	------	------	------	------	------	------	------	------

↑  
p\_lpString2

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x56	0x78	0x90	0x00	0x11	0x22
0x00	0x00								

↑  
concatpoint

# Root Cause

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            *concatpoint = lpString2_i2;
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x00 == 0x00  
lpString2\_i3 : 0x00 == 0x00

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0x12	0x34	0x56	0x78	0x90	0x00	0x11	0x22	0x00	0x00
------	------	------	------	------	------	------	------	------	------

p\_lpString2 ↑

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x56	0x78	0x90	0x00	0x11	0x22
0x00	0x00								



concatpoint



# Root Cause

```
if ( *lpString1 == (CHAR)0xFE && lpString1[1] == (CHAR)0xFF )
{
    len_lpString1 = (int)custom_strlen(lpString1);
    p_lpString2_i2 = lpString2 + 2;
    concatpoint = &lpString1[len_lpString1];
    do
    {
        do
        {
            lpString2_i2 = *p_lpString2_i2;
            p_lpString2_i2 += 2;
            *concatpoint = lpString2_i2;
            concatpoint += 2;
            lpString2_i3 = *(p_lpString2_i2 - 1);
            *(concatpoint - 1) = lpString2_i3;
        }
        while ( lpString2_i2 );
    }
    while ( lpString2_i3 );
}
```

len\_lpString1 : 4  
lpString2\_i2 : 0x00 == 0x00  
lpString2\_i3 : 0x00 == 0x00

Base URL

0	1	2	3	4	5	6	7	8	9
0xFE	0xFF	0x41	0x41	0x00	0x00	0x42	0x42	0x42	0x42

Relative URL

lpString2 →

0x12	0x34	0x56	0x78	0x90	0x00	0x11	0x22	0x00	0x00
------	------	------	------	------	------	------	------	------	------

Out Of Bound Read

Concat URL

lpString1 →

0xFE	0xFF	0x41	0x41	0x56	0x78	0x90	0x00	0x11	0x22
0x00	0x00								

Out Of Bound Wrtie

Heap Buffer Overflow

concatpoint

p\_lpString